Investigating User Comprehension and Risk Perception of Apple's Touch ID Technology

Conference Paper · August 2017

DOI: 10.1145/3098954.3098974

CITATIONS
8

READS
163

3 authors:

Yousra Javed
Illinois State University
30 PUBLICATIONS **185** CITATIONS
SEE PROFILE

Mohamed Shehab
University of North Carolina at Charlotte
102 PUBLICATIONS **1,885** CITATIONS
SEE PROFILE

Emmanuel Bello-Ogunu
University of North Carolina at Charlotte
10 PUBLICATIONS **77** CITATIONS
SEE PROFILE

Investigating User Comprehension and Risk Perception of Apple's Touch ID Technology

Yousra Javed
UNC Charlotte
yjaved@uncc.edu

Mohamed Shehab
UNC Charlotte
mshehab@uncc.edu

Emmanuel Bello-Ogunu
UNC Charlotte
ebelloog@uncc.edu

ABSTRACT

Apple's Touch ID serves as an alternative to PIN/password for unlocking Apple devices, signing into third party iOS applications, and authorizing purchases on the iTunes Store by simply tapping a registered finger on the home button.

This paper investigates the user comprehension and risk perception of Apple's Touch ID technology. We conducted two user studies to assess user perceptions in three domains: 1) Touch ID authentication process for third party applications; 2) fingerprint access and storage; and 3) ease of circumventing Touch ID. We first conducted an in-person study with 30 participants and then validated our findings through an online study over Amazon Turk on a larger sample of 125 participants. Our findings show that Touch ID users are unaware of the Touch ID authentication process for signing into applications, and have incorrect perceptions regarding the storage/access of their registered fingerprint before and after Touch ID authentication.

KEYWORDS

Touch ID, User perceptions, Fingerprint authentication

1 INTRODUCTION

Smartphones, used widely today, contain massive amounts of personal data including contacts, photos, and credit card information. This poses a serious threat to the security and privacy of user information stored on their device.

Many smartphone owners do not lock their devices with a passcode since it gets in the way of their experience [9]. Fingerprint authentication has been recently introduced for this very reason as a fast and secure alternative to PIN/ passcode on smartphones. The first smartphone vendors to add fingerprint scanners to their handsets include Samsung, Huawei, and HTC. Apple introduced Touch ID in 2013, and was the first to implement fingerprint authentication into the operating system. Apple's iPhone 5S is the first phone on a major US carrier since then to feature the Touch ID technology [8].

Touch ID not only enables users to unlock their devices, but also allows users to authenticate themselves to third party applications, and to authorize application purchases. The third party applications use the Local Authentication Framework to verify that the provider of the fingerprint is the owner of the device. Upon verifying, the application retrieves the username and password from the keystore [2]. Due to the fact that a fingerprint is used during the authentication procedure, a misconception that Touch ID is used to authenticate the users in the applications is introduced. Moreover, since the application sits inside the phone, there is an assumption that application authentication using Touch ID is the same as unlocking the phone.

Touch ID authentication takes place on the Apple device. The fingerprint data is only stored on the Secure Enclave of the device's chip, and not on Apple servers or iCloud [1]. The fingerprint data is never shared with or accessed by any application on the device, and it never leaves the device.

Touch ID adds a layer of security to the Apple device if PIN/ passcode is not used to lock the device. Moreover, the multiple finger registration functionality in Touch ID improves the usability of Touch ID. However, the fact that Touch ID allows registration of up to five fingers, can allow an adversary to unlock the device using their own fingerprint. This is possible in a scenario where an adversary is able to eavesdrop on the user's passcode, using which the adversary can register their own fingerprint to allow them to unlock the device in the future, even if the passcode is changed. Similarly, the user's fingerprint can be photographed from a glass surface, to create a fake fingerprint that could unlock a Touch ID enabled device [5].

In this paper, we investigate the user comprehension and risk perception of Apple's Touch ID technology. We conduct user studies to assess user perceptions in three domains: 1) Touch ID authentication process for third party applications 2) fingerprint access and storage and 3) ease of circumventing Touch ID.
We conduct an in-person study with 31 participants, and an online study using Amazon Mechanical Turk (MTurk) with 125 participants to corroborate our findings from the in-person study. Our findings show that users are unaware of the Touch ID based authentication process for third party applications, and have incorrect perceptions regarding the storage/access of their registered fingerprint before and after Touch ID authentication.

2 BACKGROUND

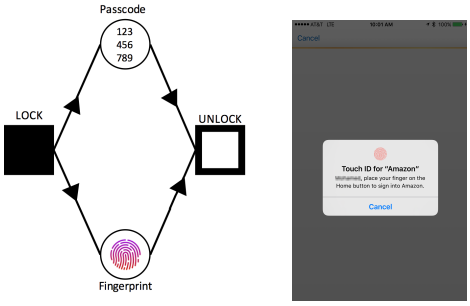
We begin this section with a description of what Touch ID is and how it is used. We then briefly explain the related hardware components and security design.

2.1 Using Touch ID

2.1.1 ***Device lock/unlock.*** Touch ID is Apple's biometric authentication mechanism that utilizes a fingerprint sensor built into

ARES '17, August 29-September 01, 2017, Reggio Calabria,Italy

ACM ISBN 978-1-4503-5257-4/17/08…$15.00
https://doi.org/10.1145/3098954.3098974



(a) Mechanisms of unlocking an Apple device

(b) Authentication in third party applications

Figure 1: Touch ID Usage

the home button of an Apple device. Its use is meant to increase security in Apple devices where a passcode (representing either a PIN or alphanumeric password) was formerly not used at all [3]. That is because configuring Touch ID requires setting a passcode. The use of Touch ID makes the authentication process faster and easier by minimizing entering a passcode. However, a passcode is still required for additional security validation. For example, when the device is restarted or when more than 48 hours have passed since the device was unlocked. Figure 1a depicts how entering a passcode and using a fingerprint are two independent mechanisms to unlock a device or be authenticated by a third party application. Enrolling a fingerprint with Touch ID involves placing the finger on the home button repeatedly, until a comprehensive fingerprint image has been captured. Touch ID can register up to five fingerprints which can be read in 360-degrees of orientation.

2.1.2 ***User authentication in third party applications.*** Touch ID is now also being used by the third party developers to authenticate registered users into their application. Banks are using Touch ID based on the assumption that the user's fingerprint is tied to the device and only the owner can unlock it. However, anyone whose fingerprint is registered on the device can unlock the device and be authenticated as the owner of these applications. Touch ID based user authentication for applications works as follows:
Step 1: User signs into the application for the first time using his username and password. The user's account credentials are then stored in the secure keystore.
Step 2: Once the user enables Touch ID for third party applications, all subsequent sign-ins to the application are done through Touch ID. The Touch ID pop up appears on the application's sign-in activity (see Figure 1b), where the user taps a registered finger on the home button, and is verified by the third party application using local authentication framework as being the owner of the device.
Step 3: If the user is verified as the owner of the device, their username and password is securely retrieved from the keystore to authenticate them.
A similar procedure is performed when authenticating the user and making purchases in iTunes Store, App Store, and iBooks Store, as well as to make Apple Pay purchases in physical stores.

2.2 Hardware & Security

Touch ID's hardware components include a laser-cut sapphire crystal, built into the home button, which acts as a sensor and protects the lens, along with a steel capacitative ring to detect the user's finger [1]. When the finger makes a contact with the ring, the sensor captures a high-resolution image from small sections of the fingerprint. This image is then converted into a mathematical representation, encrypted, and carried over a hardware channel to a "Secure Enclave" on the device's chip for authentication. This Secure Enclave is the only location where the fingerprint data is stored, and not on any Apple servers or iCloud, nor within any application. Additionally, the fingerprint authentication process only takes place locally on the device, not within any application. During this process, the captured fingerprint data is compared with the stored fingerprint data to determine a match. If the fingerprint is determined as a match, then a "yes" token is released, and authorization is enabled. Otherwise, a "no" token is released, resulting in an unsuccessful attempt. Up to five unsuccessful fingerprint matches are allowed before the device prompts for a passcode to be entered, and the user cannot proceed until doing so.

3 RELATED WORK

The literature most relevant to our work is regarding users' smartphone locking behaviors. Egelman et al. conducted a series of qualitative experiments to examine how users choose to employ locking mechanisms, ranging from PIN/passcode, and pattern to fingerprints [6]. They found a strong correlation between the use of locking methods and risk perceptions, with a major reason for not locking smartphones including not believing there was any data worth protecting. This demonstrated that many users did not understand the extent to which their stored data could pervade their online and offline identity. Van Bruggen et al. evaluated the ability to influence change in pattern-based and text-based locking mechanisms [10]. While two-thirds of those sampled, secured their devices without prior interventions, any induced interventions had only limited impact, particularly when security was the intended source of influence. Karthikeyan et al. investigated locking behaviors specifically surrounding Touch ID as compared to PINs. This was done in order to determine whether fingerprint-based authentication is more likely to gain greater adoption than traditional PINs [7]. They found that the usability of fingerprint-based authentication over PIN-based could be a significant influencer to increased adoption of locking behavior, compared to the population of people who avoid locking at all. Cherapau et al. conducted a related study on the impact of Touch ID on iPhone passcodes [4]. While there is an expectation that using Touch ID allows users to employ stronger passcodes, results showed that they do not take advantage of this [3].

4 HYPOTHESES AND METHODOLOGY

Touch ID allows a fingerprint to be associated with a user's device, whereas a passcode is normally associated with a user's account on specific third party applications. When Touch ID is used to authenticate with these applications, a mental model, that the fingerprint and passcode are interchangeable methods of authentication is introduced. Herein lies the root of potential misconceptions regarding

the use and risk associated with Touch ID. While this might be considered a safe assumption due to the fact that the applications sit on the device, in reality the owner of the device is not necessarily always the user associated with all the applications on a device. Moreover, all of the fingerprints registered on the device may not belong to the actual owner of the device. Hence, we have observed that it is possible for a user, who may or may not be authorized to use the device, to be authenticated as an intended user of an application on the device if their fingerprint is registered with Touch ID. Consequently, we formulated the following hypotheses in order to drive our investigation of whether Touch ID users lack comprehension and risk perception of Touch ID technology:

H1– Users are unaware of how the fingerprint is being used during Touch ID based authentication process for third party applications

H2– Users are unaware of where their fingerprint is stored and how it is accessed during Touch ID based authentication

H3– Users perceive that it is not possible for someone other than the owner to unlock the Touch ID-enabled device and make a purchase with their fingerprint

In order to evaluate our hypotheses, we first conducted an in-person study, and then an online study in order to corroborate our findings from the in-person study.

4.1 In-Person Study

4.1.1 ***Task 1 - Fingerprint enrollment and passcode creation.*** We provided participants with an iPad mini 4 device running iOS 9.2.0 and asked them to configure Touch ID by creating a passcode and enrolling a fingerprint.

4.1.2 ***Task 2 - Perceptions about Touch ID based unlock/ authentication, fingerprint access/storage, and ease of circumvention*** . After completing the first task, the participants completed a short survey that comprised of questions assessing demographics, security consciousness, and familiarity with Touch ID. Participants were then asked to install the Amazon application (version 5.4.0 at the time of our study) which implements TouchID to allow users to authenticate into their Amazon account. The participants signed up for or logged into their Amazon account, and performed the steps involved in an in-app purchase using Touch ID. We used the Amazon application in our study. Once the prompt for Touch ID was displayed prior to making a payment on Amazon, as seen in Figure 1b, participants completed another set of questions directly related to the purchase scenario, which evaluated their understanding of how the Touch ID was used in device unlock and Amazon authentication, how the fingerprint was being stored/accessed during the purchase transaction, and how easy it was for an intruder to circumvent Touch ID to unlock the device and make purchase.

4.1.3 ***Task 3 - Fingerprint management.*** The third task was related to participant perceptions regarding fingerprint management. We told the participants that we shoulder surfed the passcode they created as part of Task 1. Therefore, we were able to unlock the iPad using their passcode and register our fingerprint to use Touch ID. Based on this attack vector information, the participants were required to answer additional questions about whether they believed we would be able to unlock the device and assume their identity, and whether changing the PIN/password on the device would prevent the attack. Once they responded, we enrolled our own fingerprint with Touch ID, demonstrated the unlocking action, asked them to change the PIN/password, and then again demonstrated the attack.

We recruited our participants through mass distribution emails and flyers around campus. Respondents were screened for eligibility based on ownership of a Touch ID enabled Apple device. The study took approximately 25 minutes to complete and each participant received a $5 Amazon gift card.

4.2 Online Study

4.2.1 ***Task - Perceptions about Touch ID based unlock/ authentication, fingerprint access/storage, and ease of circumvention.*** The online study participants only completed Task 2 of the in-person study. Each participant first answered a set of questions about demographics, security consciousness, and familiarity with Touch ID and then observed a short video demonstrating the same scenario that the in-person participants had to complete, i.e., logging into Amazon account and making a purchase using Touch ID. After viewing the video, the online participants answered a set of questions related to the demonstrated scenario. These questions evaluated their understanding of how the Touch ID was used in device unlock and Amazon authentication, how the fingerprint was being stored/accessed during the purchase transaction, and how easy it is for an intruder to circumvent Touch ID to unlock the device and make purchase.

To ensure participants owned a Touch ID-enabled device, they were required to complete a verification task at the end of the study. This task required each participant to provide (1) a picture of their iPhone/iPad, taken using the front-facing camera in front of a mirror, and (2) a screenshot of their iPhone/iPad's lock screen with the masked PIN/password entered [4].

We recruited our participants from Amazon Mechanical Turkand set up our study as an HIT. We excluded the participants who failed the attention check questions, or the Touch ID enabled device ownership verification task. The HIT took approximately 20-25 minutes to complete, for which each worker was paid a reward of $0.50.

5 RESULTS

5.1 Demographics

A total of 31 participants completed the in-person study, and 155 participants completed the online study. Out of the 155 participants in our online study, we selected the responses of 125 participants after eligibility verification. A breakdown of demographics from the two studies can be seen in Table 1. These covered gender, ethnicity, age, and education.

5.2 Hypothesis 1

Touch ID users are not aware of how the fingerprint is being used in the Touch ID based authentication for third party applications

The Touch ID authentication process only takes place on the device. This means that the locally stored fingerprint data is used to verify an authorized user, and in doing so, the user's associated

Table 1: Demographics of in-person and online study

Demographics		*% Participants (in-person study)*	*% Participants (online study)*
Gender	Female	22.58	53.6
	Male	77.41	46.4
Highest level of completed education	Bachelor degree	41.9	43.2
	Associate degree	16.1	16
	High school	25.8	20.8
	Graduate degree	16.1	20
Ethnicity	Black/African-American	0	8.8
	Asian/Pacific Islander	54.83	16.8
	Hispanic	9.67	5.6
	White/Caucasian	35.48	68.8
Age	18-35	100	76
	35-50	0	20.8
	>=50	0	3.2

PIN/password is provided to the device or application for authentication. Therefore, to the device or any application requiring authentication, it is technically as if a PIN/password was entered in the first place. With this particular hypothesis, we are specifically addressing participants' understanding of the role of fingerprint during authentication, i.e., that they believe that fingerprint authentication is equivalent to PIN/password authentication, and that their fingerprint data is being accessed by applications to authenticate participant's identity, when in fact, neither of these are the case.

Table 2: Participant perceptions regarding Touch ID authentication process in the in-person and online study

Questions & Responses		*% participants (in-person study)*	*% participants (online study)*
Is being authenticated by your fingerprint the same as by your username/password?	Yes	56.6	61.6
	No	30	27.2
	I don't know	13.3	11.2
Is your fingerprint being used by Amazon to authenticate you during this transaction	Yes	60	77.6
	No	26.66	14.4
	I don't know	13.33	8

Table 3: Participant perceptions regarding fingerprint storage before/after, and fingerprint access during the Touch ID-based Amazon in-app purchase transactions

Question	*iPhone (%) In-Person*	*Other (%) In-Person*	*iPhone (%) Online*	*Other (%) Online*
Where is your fingerprint stored BEFORE purchase?	53.33	46.66	56	44
Where is your fingerprint stored AFTER purchase?	46.66	53.33	48	52
Who accesses your fingerprint DURING purchase?	46.66	53.33	41	58

To evaluate this hypothesis, we analyzed responses to two questions from the post-survey of the in-person study: (1) Is being authenticated by your fingerprint the same as authenticating by your username/password? and (2) Is your fingerprint being used by Amazon to authenticate you during this transaction? For both of these, the possible responses were "Yes,", "No," and "I don't know". Table 2 shows the participant responses to these questions. Recomputing the variables in order to reduce responses to two levels, we combined the "No" and "I don't know" responses into one. Since each of these questions could be considered a single categorical variable with two groups, this required a single-sample non-parametric test. Consequently, we used a Chi-square goodness-of-fit test in order to determine whether the distribution of cases for each question follows a known or expected distribution. For this expected distribution, we hypothesized that an equal proportion of participants would believe that fingerprint authentication was equivalent to PIN/password authentication, and that Amazon did access their fingerprint data for authentication. Since no standard or known proportion of Touch ID users exists for these cases, we used the probability that at least half of users would hold incorrect assumptions about Touch ID authentication as a reasonable assumption. We use the same expected distribution for other Chi-square goodness-of-fit tests conducted.

We hypothesized that approximately half of our participants would believe that fingerprint authentication was equivalent to PIN/password authentication, and also believe that Amazon did use their fingerprint to authenticate them.

Chi-square goodness-of-fit test on perceptions regarding authentication with fingerprint being the same as username/password showed that 50% of the in-person study participants incorrectly perceive/or are unsure that being authenticated by fingerprint on a Touch ID enabled device is the same as being authenticated by username/password. Therefore, these perceptions do not differ significantly from the hypothesized (50%,50%) values that we supplied ($\chi^2(1) = .290$, p = .590). However, more than 50% of the online study participants had the incorrect perception ($\chi^2(1) = 9.8$, p = 0.001745).

Similarly, Chi-square goodness-of-fit test on perceptions of whether fingerprint was being used by Amazon to authenticate the participant during the purchase transaction showed that 50% of the in-person study participants incorrectly perceive/or are unsure that Amazon has access to their fingerprint data in order to authenticate them during the purchase transaction. Therefore, these perceptions do not differ significantly from the hypothesized (50%,50%) values that we supplied ($\chi^2(1) = 1.581$, p = .209). However, more than 50% of the online study participants had this incorrect perception ($\chi^2(1) = 45$, p = $1.97 \times e^{-11}$).

5.3 Hypothesis 2

Touch ID users are not aware of where their fingerprint is stored and how it is accessed during authentication

Going beyond users' understanding of what it means to be authenticated using Touch ID, we hypothesized that users are not clear on how the process works with regards to where their fingerprint data is stored and how it is accessed. Specifically, we hypothesized that at least half of Touch ID users likely believe that their fingerprint data is stored beyond the Apple device itself, and that it is accessed by parties beyond the device. In the case of our user study, the provided scenario involved using Touch ID to make a purchase in the Amazon Application, and so the study questions related to

fingerprint storage were (1) Where is the fingerprint stored *before* the payment transaction? and (2) Where is the fingerprint stored *after* the transaction? For these questions, the possible responses included iPhone/iPad, iCloud account, Apple server, and Amazon server; participants could select all that they believed applied. We recoded these responses into two groups: iPhone/iPad only, and Other (iPhone/iPad and/or other server(s)) (see Table 3). This was done since we were mainly interested in determining what percentage of the participants realized that the data was stored on the iPhone/iPad only versus any other location(s).

We evaluated each set of responses as a single categorical variable with two groups, which required the Chi-square goodness-of-fit test. We also evaluated these sets of responses as two related groups (*before* and *after*) with the same dichotomous dependent variable (storage location). In other words, we sought to determine whether the proportion of participants who believed the fingerprint was stored on the iPhone/iPad only *before* the transaction significantly decreased *after* the transaction. This comparison required the use of McNemar test—a nonparametric test specifically for two related sample cases. Additionally, regarding the matter of fingerprint access, we asked participants (3) Who has access to your fingerprint *during* the payment transaction? Recoding this third set of responses into two groups and treating it as a single categorical variable with two groups, we again conducted the Chi-square goodness-of-fit test.

The Chi-square goodness-of-fit test result for the question regarding fingerprint storage *before* an Amazon transaction, was not statistically significant for the in-person ($\chi^2(1) = .806$, p = .369) and online responses ($\chi^2(1) = 0.76923$, p = 0.3805), nor was the result significant for fingerprint storage *after* the transaction for the in-person ($\chi^2(1) = .032$, p = .857) and online responses ($\chi^2(1) = 0.2$, p = 0.6547). This means that for both of these, we can not reject the null hypothesis, and confirm that our estimated proportion of users who correctly understand where the fingerprint is stored compared to those who do not is accurate at 50%/50%. For the McNemar test conducted to determine if there was a significant change in that proportion from *before* to *after*, the transaction resulted in a p-value greater than 0.05 for both the in-person and online responses, and therefore deemed not statistically significant.

Lastly, for the third question regarding fingerprint access *during* the transaction, the Chi-square goodness-of-fit test result was not statistically significant in the in-person ($\chi^2(1) = .032$, p = .857) or the online responses ($\chi^2(1) = 3.528$, p = 0.06034). Therefore, we again confirm that we were correct in assuming that the proportion of users who are not aware of how authentication with Touch ID works is approximately 50%; these are the users who perceive the fingerprint to be accessed by iPhone/iPad and/or other entities (Apple server, iCloud server, Amazon server).

5.4 Hypothesis 3

Touch ID users perceive that it is not possible for someone other than the owner to unlock the Touch ID-enabled device and make a purchase with their fingerprint

This hypothesis addresses users' lack of understanding of how someone besides themselves can take advantage of Touch ID to act as an authorized user and unlock owner's device, or, in the case of our scenario, potentially make a purchase through device owner's Amazon account. Evaluating this hypothesis consisted of analyzing responses to four questions, each with a slightly different variation, as seen in Table 4. These questions deal with who the device owner is, who the Amazon account holder is, and whose fingerprint is being used. For each, the participant was asked whether it would be possible to make a purchase. Each of these questions were evaluated using the Chi-squared goodness-of-fit test.

Chi-square goodness-of-fit test on perceptions of whether a stranger could use their own fingerprint to make a purchase on the Touch ID enabled device owner's device using the owner's Amazon account showed that more than 50% of the participants incorrectly perceive/or are unsure that a stranger cannot make a purchase in this scenario, while the rest perceive it to be possible. This was the case for both the in-person and the online study. Therefore, these perceptions differ significantly from the hypothesized (50%, 50%) values that we supplied (for in-person: $\chi^2(1) = 17.065$, $p < .0001$; for online: $\chi^2(1) = 84.872$, $p = 2.2 \times e^{-16}$).

Similarly, Chi-square goodness-of-fit test on perceptions of whether a stranger could use the Touch ID enabled device owner's fingerprint to make a purchase using the owner's Amazon account on the owner's device showed that more than 50% of the participants incorrectly perceive/or are unsure that a stranger cannot make a purchase in this scenario, while the rest perceive it to be possible. Therefore, once again, these perceptions differ significantly from the hypothesized (50%, 50%) values that we supplied in both studies (for in-person: $\chi^2(1) = 5.452$, p = .020; for online: $\chi^2(1) = 60.552$, $p = 7.166 \times e^{-15}$).

Chi-square goodness-of-fit test on perceptions of whether a stranger could use the Touch ID enabled device owner's fingerprint to make a purchase using the owner's Amazon account on the stranger's device again showed that more than 50% of the participants correctly perceive that a stranger cannot make a purchase in this scenario, while the rest perceive it to be possible or are unsure. Therefore, these perceptions differ significantly from the hypothesized (50%, 50%) values that we supplied (for in-person: $\chi^2(1) = 17.065$, $p < .0001$; for online: $\chi^2(1) = 78.408$, $p = 2.2 \times e^{-16}$).

Similarly, Chi-square goodness-of-fit test on perceptions of whether a stranger could use their fingerprint to make a purchase using the participant's Amazon account on the stranger's phone again showed that more than 50% of the participants correctly perceive that a stranger cannot make a purchase in this scenario, while the rest perceive it to be possible or are unsure. Therefore, these perceptions differ significantly from the hypothesized (50%, 50%) values that we supplied (for in-person: $\chi^2(1) = 14.226$, $p < .0001$; for online: $\chi^2(1) = 84.872$, $p = 2.2 \times e^{-16}$).

Lastly, we demonstrated a scenario where we took advantage of Touch ID to act as an authorized user on the device. There were additional survey questions evaluated here, based on this scenario. We asked them whether they believed (1) we could unlock the device and potentially make a purchase without their PIN/password if our fingerprint was registered and (2) that by changing the PIN/password, they would be able to protect against a stranger completing this action with a fingerprint already registered.

We conducted a Chi-squared goodness-of-fit test on the two separate sets of responses. For the first question, we found that

the result was significant ($\chi^2(1) = 7.258$, p = .007), meaning it differed from the hypothesized proportion. This is what we expected, however, as we anticipated most participants would realize this was possible, and so our 50%/50 % proportion would not hold here. For the second question, however, the result of the goodness-of-fit was not significant ($\chi^2(1) = 1.581$, p =.209), meaning our expected proportion of those who would incorrectly assume a PIN change would help was indeed about 50%. We also conducted a McNemar test between the two sets of responses to determine whether the proportion of participants who believed we could bypass Touch ID on their device with our fingerprint would decrease based on the change in PIN on the device. This test resulted in a p-value of .035, which confirmed that the proportion did decrease, meaning a larger proportion of participants incorrectly believed that changing the PIN would solve the demonstrated issue.

5.5 Limitations

While our results were significantly positive, our studies were not without limitations. For example, the sample of participants for both the in-person and online study were in the age range of 18-35, which arguably limits how generalizable our results are overall. Along those lines, the participants in the online study who completed the HIT might not necessarily represent the general iPhone/iPad users. Additionally, we suspected that the other data we collected, such as duration of Touch ID, technical expertise, or proficiency as iOS developers, may have had some influence on the perceptions that users have regarding Touch ID. For both studies, however, the homogeneity of our sample with respect to these variables was such that we were unable to make a proper evaluation of the impact that varying levels of these factors may have.

6 DISCUSSION

It is clear from our results that participants' comprehension of how Touch ID works is somewhat misguided, such that it may provide an undue sense of increased security. Users perceive that Touch ID is more secure than other authentication mechanisms, even without properly understanding how it works or where this data is stored. This perception of decreased risk could be dangerous, particularly for the many users who already underestimate the level of sensitive and personally identifiable information that is stored on their devices. Given that the notion of biometric authentication relies on something you are (in this case, your fingerprint), which is generally harder to spoof than something you have (like a smart card) or something you know (like a PIN or password), a plausible reason for users' assumption that Touch ID is secure enough could be based on the fact that they believe their fingerprint cannot be replicated by anyone else. However, the way Touch ID is designed, there is no association with a specific fingerprint and the actual original owner of a device. To the device, all fingerprints stored on a device are considered authorized, whether they belong to one person or to many. Whether intended or not, multiple people could have the same level of privilege when it comes to accessing the device and using the features that require authentication. Hence, it may take more than user awareness, but also system-level changes to Touch ID in order to match users' mental model and ensure their security and privacy.

Table 4: Responses to survey questions regarding perceptions on the ease of getting into a Touch ID-enabled device and making a purchase

Questions & Responses		*In-person (%)*	*Online (%)*
Can someone use HIS/HER fingerprint to make a purchase with YOUR Amazon account on YOUR iPhone/iPad?	No	80	84
	Yes	16.66	5
	I don't know	3.33	11
Can someone use YOUR fingerprint to make a purchase with YOUR Amazon account on YOUR iPhone/iPad?	No	53.33	65
	Yes	30	14
	I don't know	16.66	21
Can someone use YOUR fingerprint to make a purchase with YOUR Amazon account on HIS/HER iPhone/iPad?	No	83.33	76
	Yes	46.66	9
	I don't know	3.33	15
Can someone use HIS/HER fingerprint to make a purchase with YOUR Amazon account on HIS/HER iPhone/iPad?	No	70	78
	Yes	16.66	5
	I don't know	13.33	17

7 CONCLUSION

Apple's Touch ID technology is one of the most widely used fingerprint authentication mechanisms on smartphones today. The user's registered fingerprints never leave the Apple device. Touch ID adds a layer of security for those who do not use PIN/password. However, due to the multiple finger registration feature, Touch ID can be easily bypassed if a weak PIN/password is used and someone is able register their fingerprint on the device. In this paper, we demonstrated that at least 50% of the Touch ID user base lacks the proper comprehension of Touch ID in relation to the fingerprint storage/access, authentication with third party applications, and the ease of bypassing Touch ID technology. Our findings show that people perceive Touch ID to be more secure than other unlock/authentication methods, are unaware of the Touch ID authentication process with third party applications, and have incorrect perceptions regarding the storage/access of their registered fingerprint before and after Touch ID authentication. We also demonstrated an attack vector showing how to bypass Touch ID during the in-person study.

REFERENCES

[1] Apple. 2015. About Touch ID security on iPhone and iPad. (2015). https://support.apple.com/en-us/HT204587.

[2] Apple. 2016. Local Authentication Framework. (2016). https://developer.apple.com/reference/localauthentication.

[3] Apple. 2016. Use Touch ID on iPhone and iPad). (2016). https://support.apple.com/en-us/HT201371.

[4] Ivan Cherapau, Ildar Muslukhov, Nalin Asanka, and Konstantin Beznosov. 2015. On the impact of touch id on iphone passcodes. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. 257–276.

[5] Chaos Computer Club. 2013. Chaos Computer Club breaks Apple TouchID. (21 September 2013). http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid.

[6] Serge Egelman, Sakshi Jain, Rebecca S Portnoff, Kerwell Liao, Sunny Consolvo, and David Wagner. 2014. Are you ready to lock?. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 750–761.

[7] Shri Karthikeyan, Sophia Feng, Ashwini Rao, and Norman Sadeh. 2014. Smartphone Fingerprint Authentication versus PINs: A Usability Study. (2014).

[8] Casey Newton. 2013. Apple's new iPhone will read your fingerprint. (10 September 2013). http://goo.gl/qDTtQL.

[9] Gerry Smith. 2013. Fingerprints Could Be Solution For Half of iPhone Owners Who Don't Lock Their Phones. (9 September 2013). http://www.huffingtonpost.com/2013/09/13/apple-locks-iphone_n_3908614.html.

[10] Dirk Van Bruggen, Shu Liu, Mitch Kajzer, Aaron Striegel, Charles R Crowell, and John D'Arcy. 2013. Modifying smartphone user locking behavior. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*. ACM, 10.